Windows Vista
操作系统最新安全特性

Microsoft Tech·Ed 2006 中国

提纲

- 系统平台
- 权限保护
- 防止有害软件和恶意入侵
- IE安全改进
- 数据保护
- 总结，与XP相比
- 局限
- 问/答

系统平台

- SDL
- Service Hardening
- 硬件保护
- 64位平台安全改进

安全软件开发

- Security Development Lifecycle (SDL)
- 第一个采用SDL进行开发的操作系统

系统服务保护：Service Hardening

- 背景：系统服务程序（System Service）被攻击次数日益增多
- 无需用户交互，即可自动运行
- 运行于“System”账号下

系统服务保护

- 服务程序运行在最低权限
- 服务程序有相应的配置文件，用以指定该服务可以执行的文件，注册表和网络行为

硬件保护

- 防止缓存溢出
- NX保护代码
- 寻址空间随机分布(ASLR)
  - Address Space Layout Randomization

64位平台

- 背景：有缺陷或恶意的驱动程序导致系统崩溃，不稳定，和安全问题
- 设备驱动程序
  - 所有的设备驱动程序都必须有数字认证
- PatchGuard
  - 不允许修改系统的核心状态（Kernel State）

权限保护

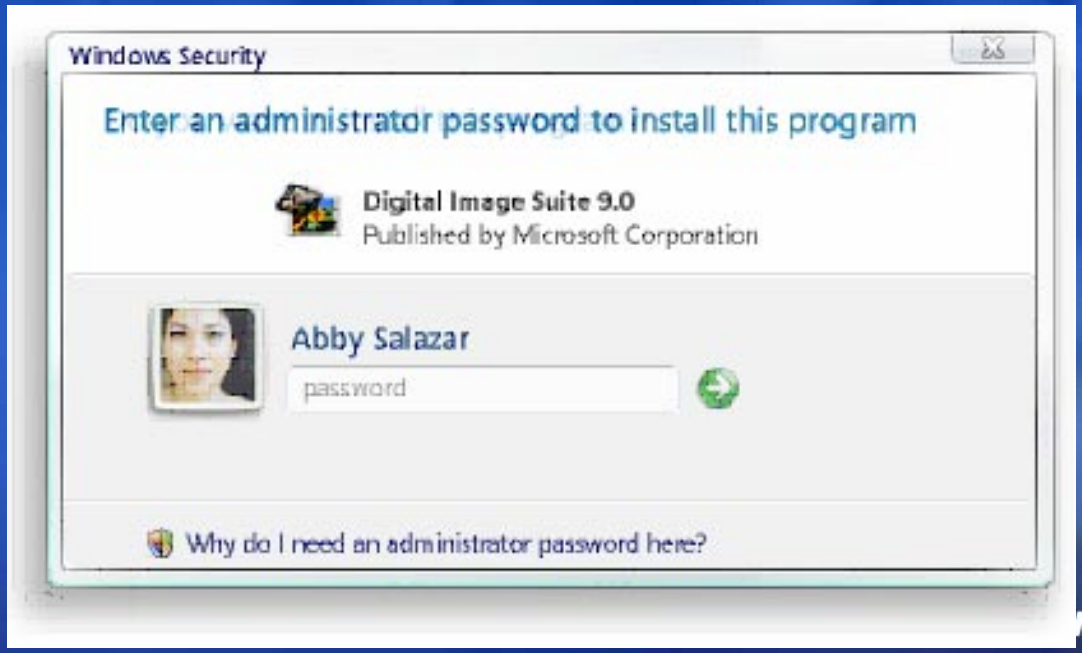
- 用户权限保护（UAP）
- 登陆体系
- Smart Card
- 网络权限保护（NAP）

用户帐号保护：背景

- 大部分用户以Admin权限登录
- 许多应用程序需要Admin权限运行
- 许多操作系统配置的修改需要Admin权限
- 计算机病毒，和间谍软件？

用户帐号保护：综述

- 用户登陆后的缺省权限是非Admin身份
- 必须通过相应的UI才能将权限升为Admin



UAP兼容性

- 应用程序和系统管理工具可在Vista的RC版本上测试
- http://www.microsoft.com/technet/windowsvista/security/uacppr.mspx

登陆体系/Smart Card

- Password 不是唯一选择 …
- 支持第三方Credential Provider
  - Biometrics
- Smart Card支持

网络权限保护（Network access protection）

- 背景
  - 一台笔记本电脑被病毒感染
  - 当该笔记本接入到公司内部网络时，病毒可以通过此电脑感染整个内部网络

网络权限保护：综述

- 任何电脑必须通过系统健康检查后才能接入公司内部网络
- 确保机器时刻保持健康状态
- 未通过系统健康检查的机器会被隔离到一个受控网络

网络权限保护

- NAP客户端程序包括在Windows Vista中
- NAP服务端程序包括在Longhorn Server中

防止有害软件和恶意入侵

- 安全中心
- Windows Defender
- 有害软件删除工具
- 防火墙

安全中心

- 第一个版本发布于XP SP2
- 提供状态信息：
  - 反间谍软件
  - Internet Explorer安全设置
  - 用户权限控制
- 支持第三方软件

Windows Defender

- 反间谍软件
  - 监控
  - 检测
  - 清除
  - SpyNet

有害软件删除工具

- XP升级到Windows Vista，先进行检测
- 不替代反病毒产品

防火墙

- 控制应用程序的对外网络连接（**application-aware outbound filtering**）
  - P2P软件
- 与系统服务保护集成
- 设置可由系统管理员通过Group Policy管理

IE安全改进

- IE 7
  - *WEB 312： 深入探讨Vista IE 保护模式*

IE浏览器：背景

- IE的安全漏洞是病毒和间谍软件传播的主要途径之一
- 针对普通用户的Phishing攻击

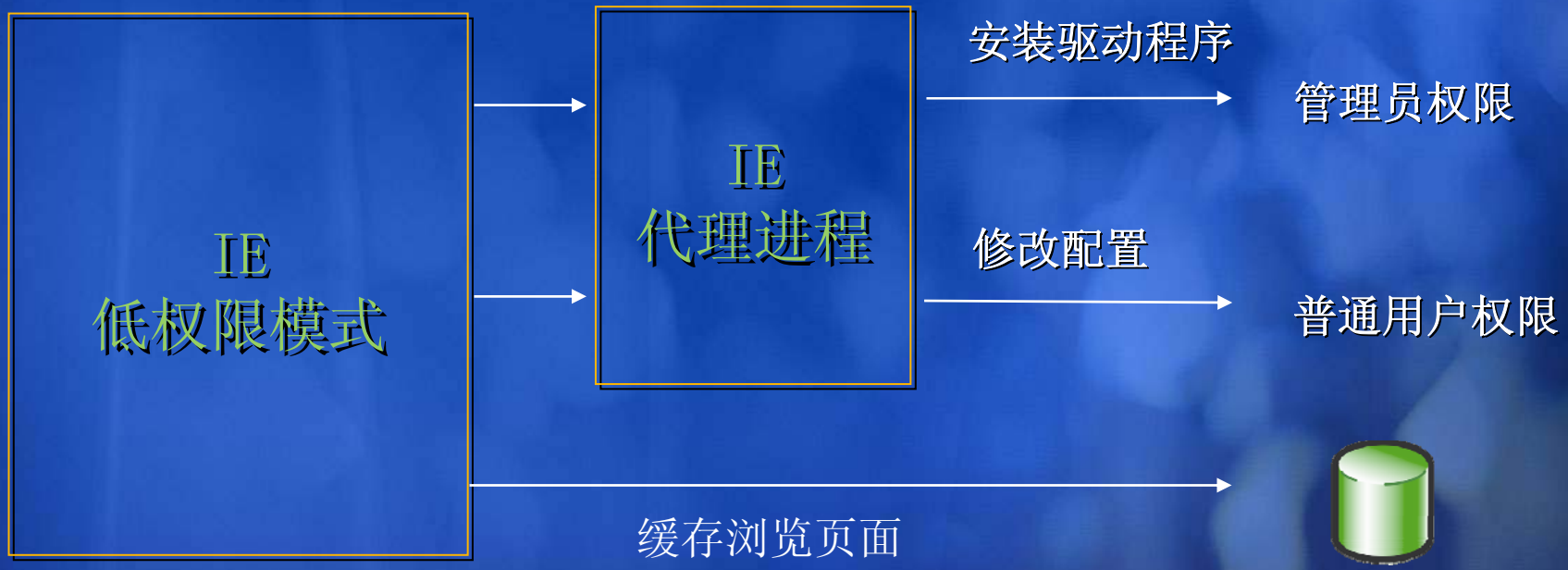
IE浏览器：目的

- IE运行于低权限模式下。以更安全访问互联网，减少安全漏洞的影响范围
- 对Phishing攻击向用户提出警告

IE：低权限模式

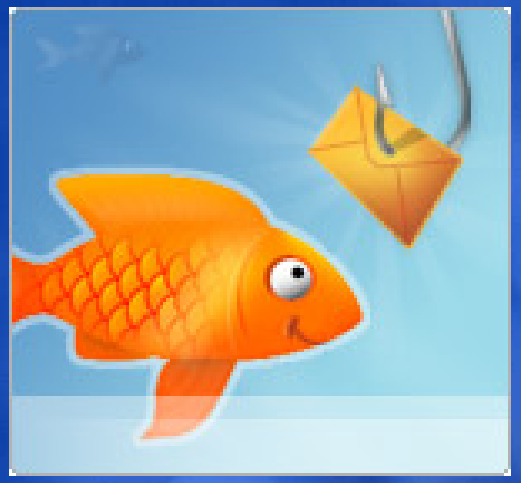
- 权限低于普通用户程序
  - 只能对文件系统的特定部分执行写操作
  - 不能对高权限的其它进程操作
- 敏感操作由代理进程（broker process）执行
  - 修改Internet设置
  - 安装ActiveX控件

IE：低权限模式架构

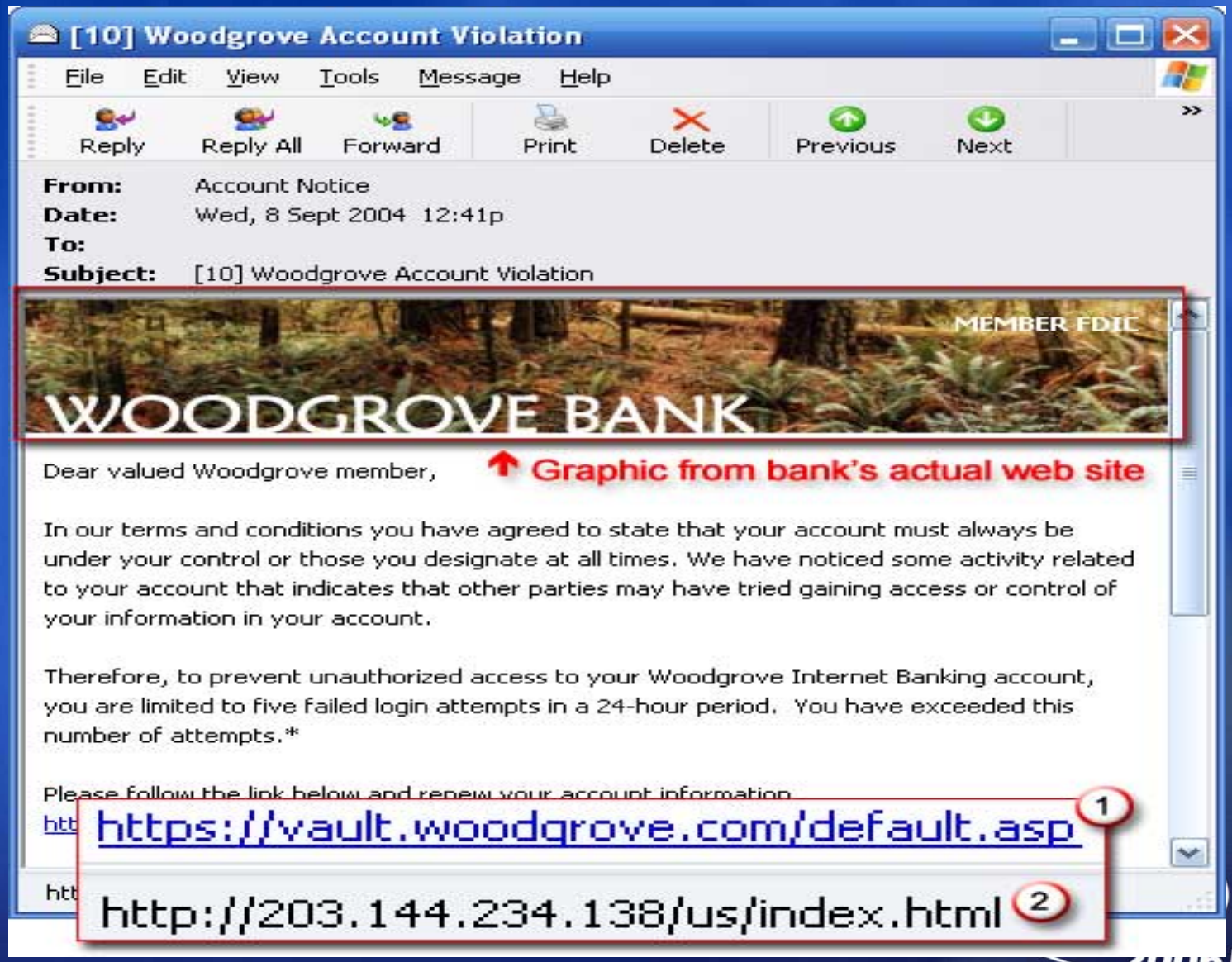


Phishing

- 复制一个官方网站的主页，诱使用户输入个人的机密信息，如银行账号，密码等等。



实例


[10] Woodgrove Account Violation
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next
From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation
MEMBER FDIC
WOODGROVE BANK
Dear valued Woodgrove member,
Graphic from bank's actual web site
In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.
Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*
https://vault.woodgrove.com/default.asp
1
http://203.144.234.138/us/index.html
2

防止Phishing攻击

- 保护URL显示
- Phishing网页过滤器（ Filter ）

数据保护

- BitLocker
- 加密文件系统
- 版权保护
- USB

BitLocker

- 安全启动
- 密码恢复程序可针对XP的数据安全保护机制进行系统离线攻击

BitLocker：目的

- 即使物理设备丢失,仍能提供对Windows客户端的安全保证
- 特别针对他人以其他OS启动试图非法获取对Windows系统文件的权限

BitLocker

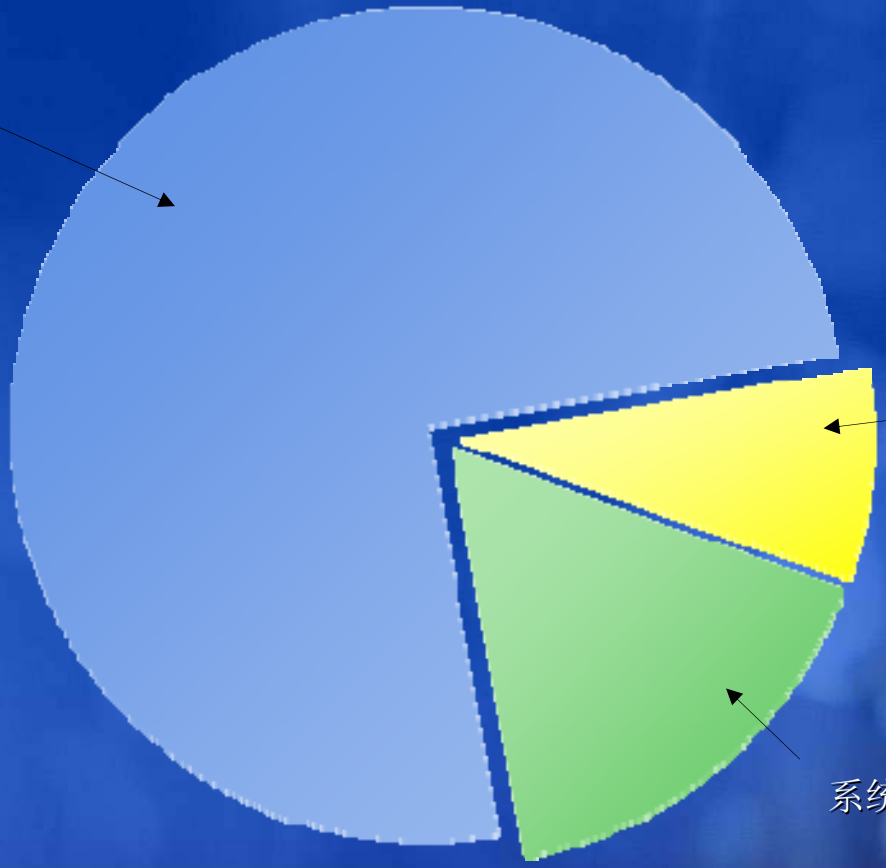
- 基于Trusted Platform Module（ TPM ）
  - http://www.microsoft.com/whdc/system/platform/pcdesign/TPM_secure.mspx
- 可锁定启动进程，要求用户提供Credential
- 硬盘全加密（Full Volume Encryption: FVM）

加密文件系统(EFS)

- Full Volume Encryption 全加密

FVE 硬盘布局

加密的 OS卷，包括：
OS，
页面文件
临时文件
数据
休眠（ hibernation）文件



MBR

系统分区包括基本引导代码

版权保护

- Office 文档
- 版权保护客户端 （RMS client）

数据保护技术总结

防范对象

- 机器其他正常用户或系统管理员? EFS
- 未授权非法用户? BitLocker™

场景	BitLocker	EFS	RMS
笔记本	●		
Branch office 服务器	●		
本地单用户文件	●		
本地多用户文件		●	
远程文件		●	
网络管理员不信赖		●	
远程office文档管理			●

USB控制

- Group Policy 可以管理对USB设备的安装

局限

- Vista的改进不能解决所有的安全问题
- 操作系统只是整个安全解决方案的一部分
- 物理设备安全
- 用户教育
  - 社会工程方式攻击

资源

Windows Vista Security:
http://www.microsoft.com/windowsvista/basics/security.mspx

Device Driver

http://www.microsoft.com/whdc/winhec/default.mspx

IE 7

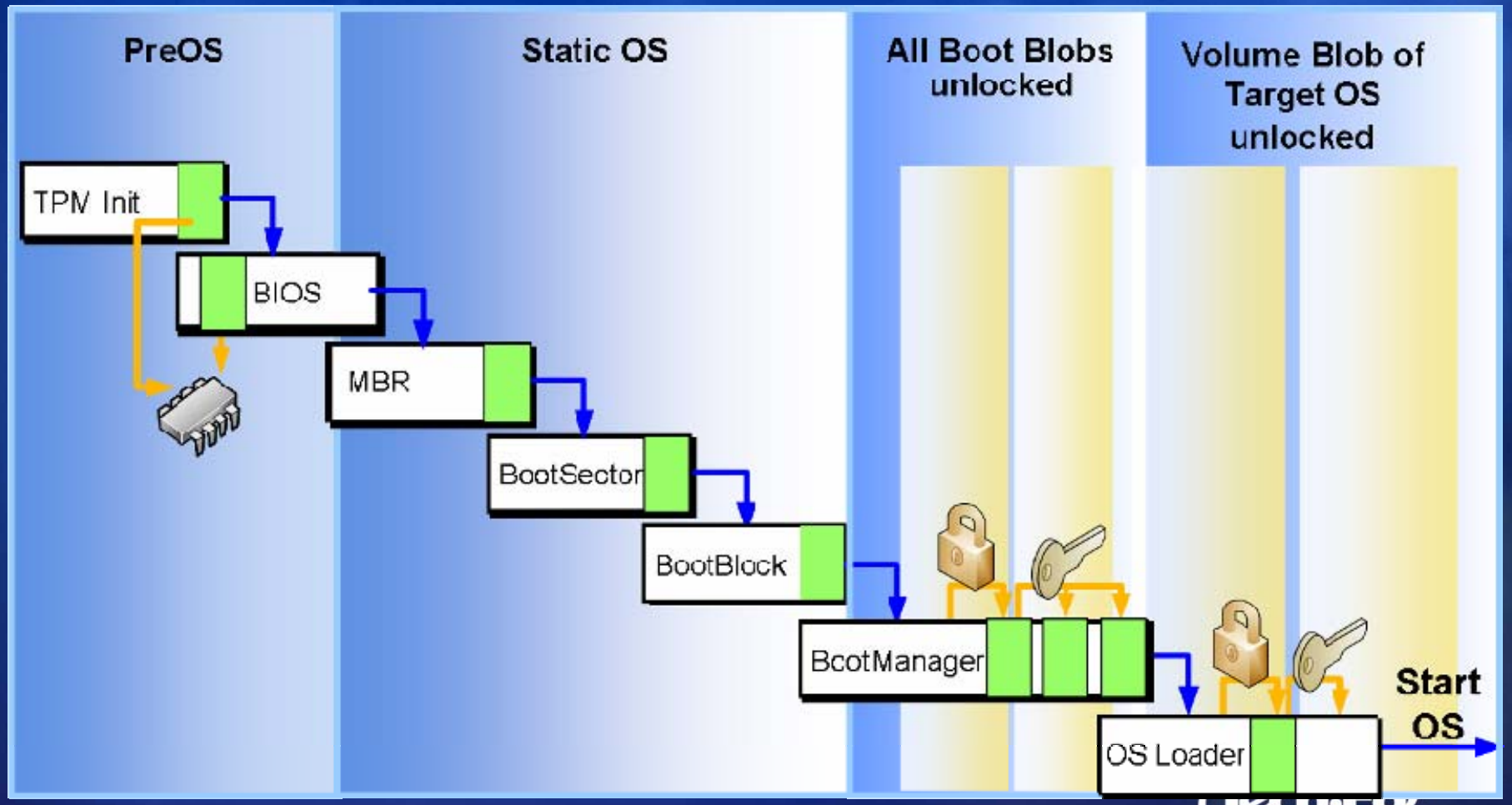
http://www.microsoft.com/windows/IE/ie7/default.mspx

信息安全Blog

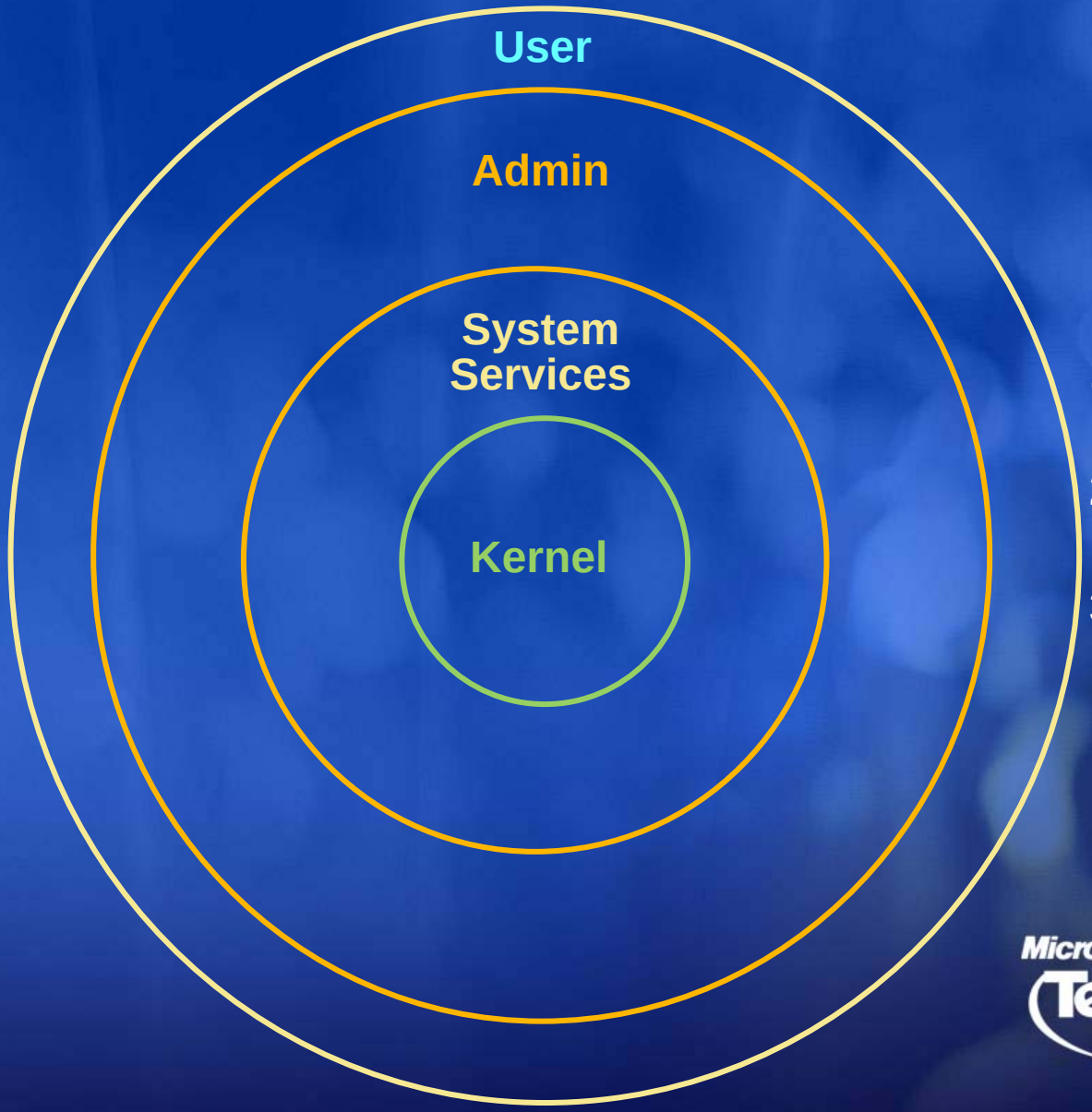
http://blogs.itecn.net/blogs/chengyun_chu

欢迎大家的反馈！

BitLocker流程

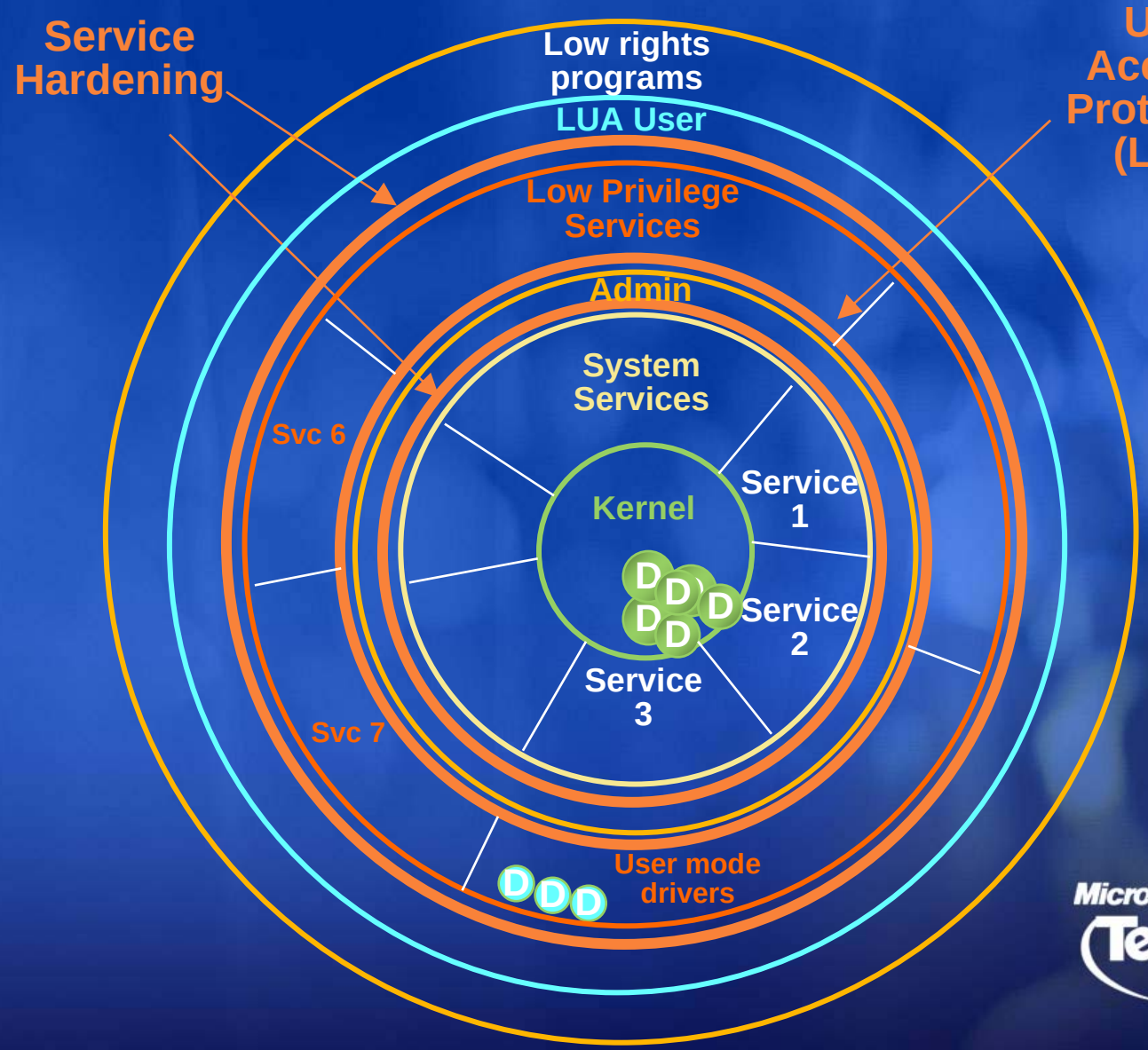


Windows XP



1. Few layers
2. Mostly privileged
3. Limited guards between layers

Vista



1. Increase # layers
2. Segment services
3. Reduce size of high risk layers

Microsoft TechEd 2006 中国